REMARKS

This Amendment is submitted in response to the Office Action mailed on February 7, 2006. Claims 21 - 38 are pending, and all stand rejected at present.

RESPONSE TO 112 - OBJECTIONS

The word "some" has been changed to "one or more." Support for the change is found in the Specification, page 3, line 6, and at other locations.

RESPONSE TO OBVIOUSNESS REJECTIONS - PART 1

Claims 21 - 34 and 38 were rejected as obvious, based on Yacobi and Menezes.

CLAIM 21

Even if References Combined,
All Claim Elements not Found - Part 1

Claim 21(c) recites "de-crypting the encrypted response using the plain text of K1." This has not been shown in Yacobi. The Office Action only asserts that Yacobi shows decrypting a response from the terminal. (Office Action, page 3, end of second -to-last paragraph.)

The Office Action does not assert that the "plain text of K1" is used in that decryption, as claimed.

Therefore, even if the references are combined, the claim recitation is not found. No decryption using "plain text of K1" as key has been shown. MPEP § 2143.03 states:

> To establish prima facie obviousness . . . **all the claim limitations** must be taught or suggested by the prior art.

This applies to claims 26(c)(ii), 32(c)(ii), and 38(h).

Even if References Combined, All Claim Elements not Found - Part 2

Background

HASHING FUNCTION

Applicant will first explain some principles involving digital cash, and then explain why Yacobi's use of digital cash does not show the claim recitations.

First, a generalized "hash function" will be explained. Assume that a message contains four decimal digits, as shown in Sketch 1, below.

MESSAGE	HASH VALUE
0000	
o o o	
1234	1 + 2 + 3 + 4 = 10
o o o	
2134	2 + 1 + 3 + 4 = 10
o o o	
3124	3 + 1 + 2 + 4 = 10
o o o	
4123	4 + 1 + 2 + 3 = 10
o o o	
9999	

Sketch 1

The message has 10,000 possible values, running from 0000 to 9999.

A hash function generally is a type of abstract of the message. In Sketch 1, the hash function is the sum of the digits in the message. The sum is called the "hash value." For the message 0000, the sum is zero. For the message 9999, the sum is 36, and so on.

Two points are significant here. One, for a hash function such as this one, which produces a hash value which is smaller than the message, **different** messages can produce the **same** hash value.

That is, the hash value is not unique to the message.

The examples in Sketch 1 illustrate this non-uniqueness: the messages 1234, 2134, 3124, and 4123 all produce the same hash value of 10. Other examples are 0505, 5050, etc.

Thus, a given message's hash value is not unique. Different messages can have the same hash value.

The second point is that the hash function is not reversible, so that the content of the message is not carried over into the hash value. Only some characteristic of the message (the sum of the digits in this example) is carried over into the hash value.

Consequently, the hash function cannot be processed to deduce the message which produced it. The examples in Sketch 1 again illustrate the point: if you are given the hash value of 10, you do not know which of the many messages produced that value.

Thus, a hash function is not a type of translation. In contrast, encryption is a type of translation: the original message can be derived from the cypher text.

Therefore, these two points illustrate the fact that a hashing function is not, in general, equivalent to encryption.

> -- The hash value is not unique to the message. This prevents reversibility, or deriving the message from the hash value. Decryption of the hash value is not possible.
>
> -- The hash function does not translate the

> message into a new form. Thus, the hash value cannot be re-translated into the message.

Of course, it may be possible to define a function which is reversible, and call it a hash function. However, such a function has not been shown in the references.

DIGITAL CASH

The phrase "ten dollars, unique serial number, bank ABC" could be used as digital cash. "Ten dollars" is the value of the digital cash, "serial number" is a unique number assigned to that piece of cash, and "bank ABC" is the bank issuing the cash.

To spend the digital cash, one transfers the phrase to a merchant, who then contacts bank ABC, and tells ABC the serial number. ABC verifies that serial number, and then authorizes ten dollars for a purchase.

However, a dishonest person could alter the phrase. Further, it may be desirable to eliminate the step of contacting ABC bank to verify the phrase.

To these ends, a hash value of the phrase can be derived. The hash value is inserted into the phrase, which now reads

> ten dollars, unique serial number,
> bank ABC, hash value.

The hash value could be the sum of the ASCII values of the characters in the phrase.

When validation of the digital cash is requested, the merchant, or the bank, computes a hash value for the phrase, using the same hash function. If the hash value produced matches the hash value contained in the phrase, the phrase is assumed to be authentic, and no alteration is assumed to have occurred.

However, a dishonest person can alter the phrase, compute the hash value for the altered phrase, and insert that new hash value into the phrase. Now the phrase could read:

1,000 dollars, unique serial number,
bank ABC, new (false) hash value

To prevent this, the hash value can be encrypted, using a private key which only bank ABC possesses, or only merchants possess, or both. Thus, the phrase becomes

ten dollars, unique serial number,
bank abc, hash value(encrypted)

Since the dishonest person lacks the private key, he cannot generate a false hash value, and then properly encrypt it.

Greater detail concerning hash functions and digital cash can be found at the following web sites:

www.iusmentis.com/technology/encryption/crashcourse/
digitalsignatures

www.aci.net/kalliste/cryptnum.htm

Application to Yacobi

Claim 21(c) recites "de-crypting the encrypted response using the plain text of K1." The Office Action cites Yacobi, column 9, line 65 - column 10, line 31 to show this.

POINT 1

However, that passage of Yacobi shows generating digital cash by a bank. The digital cash is described in column 10, lines 14 - 16, and an example of a 550-bit number is given.

Yacobi then states that a hash value is derived from the 550-bit number. The bank then encrypts the hash value, using its private key. (Column 10, lines 22 - 25.) The encrypted hash value is then transferred to the customer's electronic wallet. (Column 10, lines 32, 33.)

Applicant points out that no decryption occurs in this passage of Yacobi. Claim 21(c) recites a de-crypting process.

Thus, the encrypted hash value of Yacobi does not correspond to the "encrypted response" in claim 21(c). That encrypted hash value is not decrypted, as claimed.

POINT 2

Claim 21(c) recites "de-crypting the **encrypted response**." No "encrypted response" is shown in this passage of Yacobi. The Office Action relies on a hash value in Yacobi to show the claimed "encrypted response." However, as explained above, a hash value is not, in general, an encrypted response. A hash value cannot be decrypted.

Nor is "de-crypting" of any "encrypted response" shown in this passage. Nor is "de-crypting" of a "response" shown in this passage.

Therefore, Applicant submits three claim elements are missing from Jacobi:

1) The claimed decryption.
2) The claimed encrypted response.
3) The claimed decryption of an encrypted response.

POINT 3

Claim 21 recites "de-crypting the encrypted response using the plain text of K1." As just explained, the Office Action treats the hash value of digital cash in Yacobi as the "encrypted response." There is no decryption of that hash value. Nor is there decryption using K1 as a key.

POINT 4

Further still, the Office Action treats the "session key" in

Yacobi as the claimed key K1. Yacobi uses that "session key" to encrypt a message which a wallet transmits to an ATM. The ATM then uses the same "session key" to decrypt that message. (Column 9, lines 47 - 61.)

However, that "session key" is not involved in Yacobi's encryption of the hash value of the digital cash. Therefore, it cannot be involved in any decryption of the hash value. Consequently, Yacobi's "session key" (supposedly the claimed K1) does not decrypt the hash value (supposedly the encrypted response).

POINT 5

Under the terms of the claim, the operations of claim 21(c) are performed in the "portable computer." However, any processing of the hash function of the digital cash in Yacobi is done **outside** the electronic wallet. The processing is done by a merchant receiving the digital cash. Thus, even if Yacobi decrypts the hash function of the digital cash (which is not the case), that operation occurs **outside** the electronic wallet.

Further, it would make no sense to perform Yacobi's decryption **within** the wallet, because any decryption is designed to verify the digital cash. It makes no sense, and there is no need, for the owner of the wallet to verify his own digital cash.

Thus, any decryption of the hash value in Yacobi (if decryption occurs) occurs **outside** the electronic wallet. That does not correspond to the claim.

CONCLUSION

Applicant submits that the rejection of claim 21 cannot stand, for at least the following reasons.

-- Yacobi shows no decrypting of an encrypted response using key K1.

-- Yacobi's hash value of the digital cash cannot qualify as the claimed "encrypted response."

-- The Office Action treats the "session key" in Yacobi as key K1. For that to be so, then Yacobi's "session key" must be used to decrypt the hash value. That is not done.

No Teaching Given for Combining References

The rationale given for combining the references is that the combination provides "a random bit sequence for a key." (Office Action, page 4, third paragraph.) However, several problems exist in this rationale.

Problem 1

This rationale is merely a restatement of a well known fact in cryptography, namely, that an ideal key is a random bit sequence. Thus, since both references are interpreted as speaking to a person skilled-in-the-art, and since they both discuss keys, they both are interpreted in light of this well known fact.

Consequently, both references impliedly state, if they do not explicitly state, that their keys are random bit sequences.

Therefore, the statement does not lead to a combination of the references. Each reference, by itself, teaches using a random bit sequence.

Problem 2

The Office Action cites Menezes as stating that the starting point for a key can be user-accessible data which is stored in the user's computer. Even if that be true, Menezes discusses other sources of a random number for use in generating a seed. (See page 172.) Those other sources do not show the claimed subject matter.

Therefore, no teaching has been given in favor of selecting one approach in Menezes, as opposed to other approaches, and then combining the one selected approach with Yacobi.

Problem 3

Claim 21(a) states that the "records" are stored in "user-accessible memory." Claim 21(b) states that the "seed" for key K1 is generated from those "records."

Thus, any user of the claimed "portable computer" has access to the "records." That is contrary to Menezes' teachings.

Menezes, in section 5.2, states that "A random bit generator requires a . . . source of randomness." Under claim 21, the "source of randomness" would be the claimed "records." Thus, under claim 21, the "source of randomness" would be "user-accessible."

But Menezes' section 5.2 also states, "The generator must not be subject to observation." Menezes is contrary to storing the "records" in "user-accessible memory," as claimed.

Thus, Menezes teaches against claim 21.

Also, Menezes' section 5.2(ii) lists some events which may be similar to those in the "records" of claim 21. But Menezes states that an "adversary" should be prevented from "observing" those events. (Menezes, section 5.2(ii), fourth sentence.) Again, that is opposite to claim 21, which states that those events are stored in "user-accessible memory."

Therefore, Menezes teaches against the recitation of claim 21 regarding user-accessibility to the records used for the seed. The Office Action has provided no rationale which overcomes Menezes' contrary teaching.

Problem 4

At least two possibilities exist in Menezes. One is that Menezes

1) stores parameters in memory and then

2) later reads the parameters, and

3) then applies the parameters as inputs to an algorithm, to produce a key.

Another possibility is that Menezes eliminates steps (1) and (2), and applies the parameters directly to the algorithm, to produce a key. That is, the parameters are not stored and then read. His page 172, "(ii) Software-based generators," provides an example. He merely observes currently existing parameters (eg, system clock), and uses the parameters as the seed.

As a simple analogy, Menezes can watch a baseball game, and use

1) the current jersey-numbers of the players on-base,

2) the current score,

3) the current inning number, and

4) the current time-of-day as his seed.

He need not store anything in memory. He merely observes events.

If the latter possibility occurs, then the recited storage of claim 21(a) is not found in Menezes.

The PTO has not shown which possibility occurs in Menezes. Therefore, claim 21(a) has not been shown in the references, even if combined.

Problem 5

Menezes, page 172, discusses at least two approaches to generating a random number: (1) a hardware-based approach, and (2) a software-based, computational, approach. The first approach is clearly irrelevant to Applicant's claims, and does not show the claimed subject matter.

No teaching has been given in favor of eliminating Menezes' first approach, and selecting Menezes' second approach.

Further, Menezes expressly states that the second approach is "more difficult" than the first. (First sentence of section entitled "(ii) Software-based generators.") Thus, Menezes teaches away from the second approach, thereby teaching away from the invention.

Further still, the section entitled "(ii) Software-based generators" repeatedly states that the parameters used to generate the random number must be kept secret. That teaches away from the claim recitation that the seed is derived from "user-accessible memory."

Problem 6

A problem similar to Problems 4 and 5 applies to Yacobi.

Yacobi shows at least two implementations, an "anonymous" and a "non-anonymous" implementation. The Office Action combines the latter with Menezes.

But no teaching has been given for selecting the latter over the former.

Conclusion

No decryption as in claim 21(c) is found in Yacobi. Yacobi encrypts a **hash value**. The user in Yacobi does not **decrypt** the hash value, because (1) the user has no need to do so and (2) in general, de-crypting hash functions is not possible, because they are one-way functions.

No decryption of a "response" as in claim 21(c) is found in Yacobi.

No decryption "using the plain text of K1" as in claim 21(c) has been shown in Yacobi.

No teaching has been given for combining the references. The rationale given is merely a well-known fact, or goal, in the art of cryptography. The references need not be combined to attain that goal. And Menezes, by himself, expressly states that the goal (random number for a seed) is desirable.

REMAINING CLAIMS

The discussion of claim 21 applies to the remaining claims in this group. Applicant further makes the following comments.

Claims 22 and 23

Claims 22 and 23 are considered patentable, based on their parents.

Claim 24

Claim 24 recites producing keys from seeds derived from user-accessible memory. As explained above, Menezes teaches contrary to this.

Claim 26

Point 1

Claim 26 recites receiving an encrypted message EM1, and decrypting EM1 using K1.

The Office Action treats the encrypted hash value of the digital cash in Yacobi as the EM1. However, as explained above, in general, it is impossible to decrypt a hash value. And the Office Action has not shown otherwise.

Again, the hash value is a type of abstract, or abbreviation, of a piece of data. For example, a hash value of a person's name may be the initials. In the case of the undersigned attorney (Gregory A. Welte), the initials, or hash value, are GAW. The name Gregory A. Welte cannot be decrypted from the hash value.

Therefore, in general, a hash value is not reversible. It cannot be decrypted to provide the original message. Thus, the claimed decrypting of EM1 is not found in Yacobi.

Point 2

The claim states that K1 is the key used to perform the decryption. No such K1 is used to decrypt the hash value of the digital cash in Yacobi.

Claim 27

Claim 27 recites:

> 27. Method according to claim 26, and further comprising:
>
> d) in connection with the second transaction,
>
> i) receiving into the portable computer an encrypted message EM2 from the external terminal, and
>
> ii) de-crypting EM2 using K2.

EM2 and K2 have not been shown in Yacobi.

The comments regarding claim 26 apply here.

User-Accessible Memory

Claim 28 states that a PDA "has no secure area." Claim 30 states that an apparatus "has no secure area." Claims 21 - 27, 30, 33, and 38 state that a seed is generated from data contained in user-accessible memory.

Yacobi states that his device is "tamper-resistant." (Column

5, lines 18, 19.)

Yacobi thus teaches against these types of recitation, contained in over 90 percent of the claims.

If a user can gain access to memory from which the seeds are derived, the device containing that memory is not "tamper resistant" as required by Yacobi.

RESPONSE TO OBVIOUSNESS REJECTIONS - PART 2

Claims 35 - 37 were rejected as obvious, based on Yacobi, Menezes, and Kawan.

Point 1

These claims state that the portable computer requires a PIN "and will not complete the transaction without the PIN."

Kawan, paragraph 30, is cited to show this recitation.

However, that paragraph states that Kawan's ATM may require a PIN. The paragraph states:

> . . . the automated teller machine verifies the smart card 20 within the personal data assistant 22.
>
> The user may be required to input . . . a PIN.
>
> Upon completion of the verification, the user can then perform transactions . . . through the personal data assistant 22 . . .

This indicates that the PIN is entered into the ATM, not into the PDA. One reason in support of this conclusion is the very last phrase in the passage above. That phrase implies that the preceding "verification" (including PIN entry) was handled by the ATM, because the phrase states that now, after the verification, the customer can utilize the PDA. That implies that the PDA was not used for the verification.

In any case, Kawan's paragraph 30 is at least ambiguous as to whether the PIN is entered into the PDA or the ATM. That is insufficient as a showing under section 103.

Point 2

No teaching has been given for combining the references. The rationale given is "to verify the user." (Office Action, page 5, fourth full paragraph.) However, several problems reside in this rationale.

Problem 1

The claims state that a PIN is entered into the "portable computer." You can "verify the user" in Kawan by entering the PIN into the ATM. Thus, the stated motivation does not lead to the claimed recitation of entering the PIN onto the "portable computer."

Problem 2

Numerous ways exist to "verify a user." A PIN is just one. The Office Action has not shown why a particular mode of verification (a PIN) should be used in pursuing the stated goal (verifying the user).

Problem 3

The combination of references is contrary to Yacobi.

Yacobi discusses an ATM. (Column 5, line 35.) Everybody knows that ATMs require PINs to be entered onto the ATM's keypad. Thus, Yacobi teaches entering a PIN onto an ATM keypad.

The PTO's citation of Kawan as showing claims 35 - 37 is contrary to this teaching. Thus, even if Kawan does teach that the PIN should be entered into the portable computer, which Applicant disputes, Kawan's teaching is contrary to Yacobi.

The PTO must provide an explanation overcoming this contradiction.

Problem 4

The PTO's position is contrary to Yacobi for another reason.

Yacobi discusses verification of the user, at column 9, line 10 et seq. Yacobi undertakes a two-step process. First, he accepts data from the digital wallet. (Column 9, line 10 - 16.) Then, he verifies the user "using traditional methods." (Column 9, lines 16 - 18."

Plainly, "traditional methods" imply requesting a PIN be entered into the ATM.

Therefore, Yacobi teaches against the claimed entry of a PIN into the portable device.

CONCLUSION

Applicant requests that the rejections to the claims be reconsidered and withdrawn.

Applicant expresses thanks to the Examiner for the careful consideration given to this case.

Respectfully submitted,

Gregory A. Welte
Reg. No. 30,434

NCR Corporation
1700 South Patterson Blvd.
WHQ - 4
Dayton, OH 45479
July 24, 2006
(937) 445 - 4956